

## **Gap Analysis Document for Information Security - Cybersecurity in EASA Part 145 Organizations**

Example Case Study Presented by Sofema Online - This document assesses compliance gaps and workload development for cybersecurity within EASA Part 145 organizations. It aligns with the Implementing Regulation (EU) 2023/203 and Part IS - Information Security.

### **Section 1: Threat Identification and Assessment**

#### **Current State:**

- **External Threats:** Organizations must document external threats (e.g., phishing, DDoS) per Regulation (EU) 2023/203, Article 4(1)(a) **【source】** .
- **Internal Threats:** Assess human error and insider risks, aligned with Annex II, Part IS.I.OR.205 of Regulation (EU) 2023/203 **【source】** .
- **Emerging Threats:** Organizations should consider IoT compromises and AI-driven attacks, as outlined in AMC1 IS.I.OR.205 **【source】** .

#### **Gaps Identified:**

- Insufficient integration of systemic vulnerability assessments.
- Lack of a structured process to evaluate supply chain cybersecurity risks.

#### **Recommendations:**

1. Conduct detailed risk assessments in line with IS.I.OR.205.
2. Utilize AMC1 IS.I.OR.200 to develop a framework for emerging threat identification.

### **Section 2: Policy Development and Documentation**

#### **Current State:**

- Policies must align with Regulation (EU) 2023/203, Article 4(1)(b), requiring comprehensive information security management systems (ISMS) **【source】**
- The Information Security Management Manual (ISMM) is crucial for defining and amending cybersecurity protocols (Annex II, Part IS.I.OR.250)  
**【source】** .

#### **Gaps Identified:**

- Missing or incomplete ISMM documentation.
- Lack of a defined amendment process for ISMS.

#### **Recommendations:**

1. Update ISMM following AMC1 IS.I.OR.250 requirements **【source】** .

2. Implement structured amendments per GM1 IS.I.OR.250 【source】 .

### **Section 3: Role Assignment and Training**

#### **Current State:**

- Assign responsibilities per Annex II, IS.I.OR.240 【source】 .
- Annual training updates are required (AMC1 IS.I.OR.240(a)) 【source】 .

#### **Gaps Identified:**

- Undefined competency requirements for ISMS roles.
- Limited cybersecurity training for contractors and third-party vendors.

#### **Recommendations:**

1. Enhance training programs based on AMC1 IS.I.OR.240(e).
2. Ensure role-specific training, referencing GM1 IS.I.OR.240 【source】 .

### **Section 4: Implementation of Technical Controls**

#### **Current State:**

- Security protocols, including firewalls and encryption, must meet AMC1 IS.I.OR.200(c) 【source】 .
- Vet vendors per IS.I.OR.220 to ensure compliance 【 source】 .

#### **Gaps Identified:**

- Inadequate deployment of automated vulnerability detection tools.
- Weak multifactor authentication protocols.

#### **Recommendations:**

1. Strengthen encryption measures following AMC1 IS.I.OR.200(c).
2. Regularly test IT systems as outlined in GM1 IS.I.OR.200(d) 【source】 .

### **Section 5: Incident Response and Management**

#### **Current State:**

- An Incident Response Plan (IRP) is mandated under IS.I.OR.220 【source】
- Regular simulations (e.g., ransomware scenarios) must test readiness (AMC1 IS.I.OR.220) 【source】 .

#### **Gaps Identified:**

- Lack of scenario-based testing for incident response.
- Inconsistent external reporting mechanisms.

#### **Recommendations:**

1. Conduct scenario-based exercises as detailed in AMC1 IS.I.OR.220(b).
2. Establish reporting protocols using IS.I.OR.230 guidelines 【 source】 .

## **Section 6: Continuous Monitoring and Auditing**

### **Current State:**

- Internal audits are required per IS.I.OR.235 to confirm compliance 【source】
- Findings should inform process improvements (GM1 IS.I.OR.235) 【source】

### **Gaps Identified:**

- Limited audit integration into cybersecurity management.
- Insufficient monitoring of third-party compliance.

### **Recommendations:**

1. Expand audit programs per AMC1 IS.I.OR.235(b).
2. Use findings to refine ISMS continuously, as outlined in GM1 IS.I.OR.260 【source】 .

## **Section 7: Annual Review and Continuous Improvement**

### **Current State:**

- Organizations must conduct annual reviews and risk reassessments per IS.I.OR.260 【Source】 .
- Continuous improvement initiatives should align with AMC1 IS.I.OR.260(a) 【source】 .

### **Gaps Identified:**

- Inadequate documentation of improvement initiatives.
- Emerging threats are not consistently reassessed.

### **Recommendations:**

1. Conduct comprehensive reviews following GM1 IS.I.OR.260(a).
2. Update security controls to address newly identified vulnerabilities 【source】

## **Section 8: Oversight of Contracted Activities**

### **Current State:**

- Contractors must comply with ISMS requirements under IS.I.OR.235 【source】 .

- Regular audits of third-party activities are essential (AMC1 IS.I.OR.235(a) 【source】 .

**Gaps Identified:**

- Insufficient oversight mechanisms for contractors.
- Lack of consistent audit schedules for third-party compliance.

**Recommendations:**

1. Strengthen contractor oversight with regular audits as per GM1 IS.I.OR.235.
2. Develop clear compliance requirements for all third-party activities 【source】

**Section 9: Documentation and Record-Keeping**

**Current State:**

- Detailed record-keeping is required for all risk assessments, training, and incidents under IS.I.OR.245 【source】 .
- Cross-referencing documentation with ISMS requirements ensures traceability (GM1 IS.I.OR.245) 【source】 .

**Gaps Identified:**

- Incomplete records of cybersecurity incidents.
- Weak cross-referencing between records and ISMS protocols.

**Recommendations:**

1. Maintain comprehensive records following AMC1 IS.I.OR.245.
2. Ensure clarity and accessibility of all documentation 【source】 .

**Summary of Findings**

This gap analysis has identified critical areas requiring improvement across the cybersecurity framework. Addressing these gaps is essential for ensuring compliance with Regulation (EU) 2023/203 and safeguarding organizational systems.

**Next Steps**

1. Implement recommendations in line with regulatory requirements.
2. Schedule a follow-up review within (State) months.